Load Balancing McAfee Web Gateway

Deployment Guide

v1.1.3

Copyright © 2015 Loadbalancer.org, Inc.

Table of Contents

About this Guide....3
Loadbalancer.org Appliances Supported....3
Loadbalancer.org Software Versions Supported....3
McAfee Web Gateway Appliances Supported....3
Benefits of Implementing a Load Balancer....4
Load Balancer Configuration Options....4
  Layer 4 (Recommended)....4
    DR Mode - Direct Server Return Mode (Recommended)....4
    NAT Mode - Network Address Translation Mode....4
  Layer 7....4
    SNAT / HAProxy Mode - Source Network Address Translation....4
  Persistence - aka Server Affinity....5
    Source IP Address (Recommended)....5
    Destination Hash....5
Web Gateway Deployment Modes....5
  1 – Proxy Mode (Recommended)....5
  2 – Transparent Routed Proxy Mode....5
Loadbalancer.org Appliance – the Basics....6
  Network Configuration....6
  Accessing the Web User Interface (WUI)....7
  Clustered Pair Configuration....8
Option 1 - Proxy Mode (Recommended)....9
  Deployment Architecture....9
  Load Balancer Configuration....10
    Create the Virtual Service (VIP)....10
    Define the Real Servers (RIPs)....11
  Web Gateway Configuration....12
    Modify the Web Gateways to accept traffic for the VIP....12
      Concept....12
      Configuring the McAfee Appliance....12
    Web Gateway Operating Mode....13
    Proxy Port Configuration....13
  Client Configuration....14
Option 2 - Transparent (Routed) Proxy Mode....15
  Deployment Architecture....15
  Load Balancer Configuration....16
    Create the Virtual Service (VIP)....16
    Define the Real Servers (RIPs)....18
  Web Gateway Configuration....19
    Web Gateway Operating Mode....19
  Router / Default Gateway Configuration....21
  Client Configuration....21
Testing & Validation....22
  Layer 4 – Current Connections....22
Technical Support....23
Appendix....24
  1 – Clustered Pair Configuration – Adding a Slave Unit....24
  2 – Loadbalancer.org Company Contact Information....25
  3 – McAfee Company Contact Information....26

About this Guide

This guide details the configuration of Loadbalancer.org appliances for deployment with McAfee's range of Web Gateway products. It includes recommended deployment topologies and also steps on how to configure the appliances.

For an introduction on setting up the load balancer as well as more technical information, please also refer to the quick-start guides and full administration manuals which are available at the following links:

Quickstart guide: http://www.loadbalancer.org/pdf/quickstartguideLBv7.pdf

Administration manual: http://www.loadbalancer.org/pdf/loadbalanceradministrationv7.pdf

Loadbalancer.org Appliances Supported

All our products can be used for load balancing McAfee Web Gateways. The complete list of models is shown below:

- Enterprise R16
- Enterprise
- Enterprise MAX
- Enterprise 10G
- Enterprise R320
- Enterprise VA
- Enterprise VA R16

For a full specification comparison of these models please refer to: http://www.loadbalancer.org/matrix.php

Loadbalancer.org Software Versions Supported

- v7.4.3 and later

  N.B. this guide includes configuration steps for v7.6 & later. For older versions of the appliance please contact loadbalancer.org sales or support

McAfee Web Gateway Appliances Supported

- All versions

Benefits of Implementing a Load Balancer

Since secure, reliable and available Internet access is essential and not just a luxury, steps must be taken to ensure 100% up time. Loadbalancer.org appliances provide the perfect solution by allowing multiple Web Gateway devices to be deployed in a load balanced and highly available cluster. Benefits include:

- **High-Availability –** If a Web Gateway fails, service is not interrupted
- **Maintenance** – Web Gateways can easily be taken out of the cluster for maintenance
- **Performance** – For additional performance simply add more Web Gateways to the cluster

Load Balancer Configuration Options

The following sections describe the various load balancer configuration methods that are possible when load balancing Web Gateways.

Layer 4 (Recommended)

DR Mode - Direct Server Return Mode (Recommended)

In this mode, traffic from the client to the Web Gateway passes via the load balancer, return traffic passes directly back to the client which maximizes performance. Direct routing works by changing the destination MAC address of the incoming packet on the fly which is very fast. This mode is transparent by default meaning that the Web Gateway sees the real client IP address and not the IP address of the load balancer.

Due to its speed, overall simplicity and effectiveness, Direct Routing (DR) mode with source IP persistence is our recommended method and can be used in both proxy mode & transparent (routed) proxy mode.

NAT Mode - Network Address Translation Mode

This mode requires the implementation of a two-arm infrastructure with an internal and external subnet to carry out the translation (the same way a firewall works). The real servers (i.e. the Web Gateways) must have their default gateway configured to be the load balancer. It offers high performance and like DR mode is transparent by default.

Layer 7

SNAT / HAProxy Mode - Source Network Address Translation

Using HAProxy in SNAT mode means that the load balancer is acting as a full proxy and therefore it doesn't have the same raw throughput as the layer 4 methods. Also, this method is not transparent by default so the real servers will see the source address of each request as the load balancers IP address. This is generally not desirable although this can be resolved in two ways; either by reading the X-Forwarded-For header that's included by default when using HAProxy, or by enabling Tproxy on the load balancer. The issues with using Proxy are that the default gateway on the real servers (i.e. the Web Gateways) must be changed to point as the load balancer and also it requires a two-arm infrastructure with two subnets which complicates the deployment.

SNAT mode does not have the raw throughput of the layer 4 solutions and is therefore not normally used for Web Gateway / Proxy load balancing deployments.

Persistence - aka Server Affinity

Persistence may or may not be required and depends on the specific Web Gateway being used. Two possible methods are described in the following sections.

Source IP Address (Recommended)

Source IP persistence is the standard method and is appropriate for most requirements. When set, clients connecting from the same source IP address within the persistence timeout period (the default is 5 mins) will always be sent to the same Web Gateway.

Destination Hash

Another option at Layer 4 is to change the load balancing algorithm (i.e. the “scheduler”) to destination hash (DH). This causes the load balancer to select the proxy based on a hash of the destination IP address. This causes session requests to be directed at the same server based solely on the destination IP address of a packet which therefore makes client connections persistent for a particular Internet host.

Since this setting is a scheduler, the way connections are load balanced will also change. However it should still provide a well balanced distribution of client sessions between Web Gateway servers.

Web Gateway Deployment Modes

There are two implementation methods that are typically used – Proxy Mode & Transparent (Routed) Proxy Mode.

1 – Proxy Mode (Recommended)

This mode requires the load balancers VIP address to be defined in users browsers. This means that the load balancer will receive client requests and distribute these requests across the back-end Web Gateways.

2 – Transparent Routed Proxy Mode

With this mode, client requests must be routed to the load balancer / Web Gateway cluster. This can be achieved by either setting the default gateway on the client PCs to be the load balancer, or by adding rules to the default gateway device. Rules would typically be configured for HTTP & HTTPS traffic on ports 80 and 443.

Loadbalancer.org Appliance – the Basics

Network Configuration

The IP address, default gateway and DNS settings can be configured in several ways depending on the version as detailed below.

Configure the IP address, Default Gateway & DNS Settings

Using the Network Setup Wizard at the console:

After boot, follow the console instructions to configure the IP address, gateway and DNS settings.

Using the WUI:

Using a browser, connect to the WUI on the default IP address/port: **http://192.168.2.21:9080**

to set the IP address use: *Local Configuration > Network Interface Configuration*
to set the default gateway use: *Local Configuration > Routing*
to configure DNS settings use: Local Configuration > Hostname & DNS

Using Linux commands:

At the console, set the initial IP address using the following command:

```
ip addr add <IP address>/<mask> dev eth0
e.g. ip addr add 192.168.2.10/24 dev eth0
```

At the console, set the initial default gateway using the following command:

```
route add default gw <IP address> <interface>
e.g. route add default gw 192.168.2.254 eth0
```

At the console, set the DNS server using the following command:

```
echo nameserver <IP address> >> /etc/resolv.conf
e.g. echo nameserver 192.168.64.1 >> /etc/resolv.conf
```

N.B. If this method is used, you must also configure these settings using the WUI, otherwise settings will be lost after a reboot

Accessing the Web User Interface (WUI)

The WUI can be accessed from a browser at: ***http://192.168.2.21:9080/lbadmin***

** Note the port number → 9080*

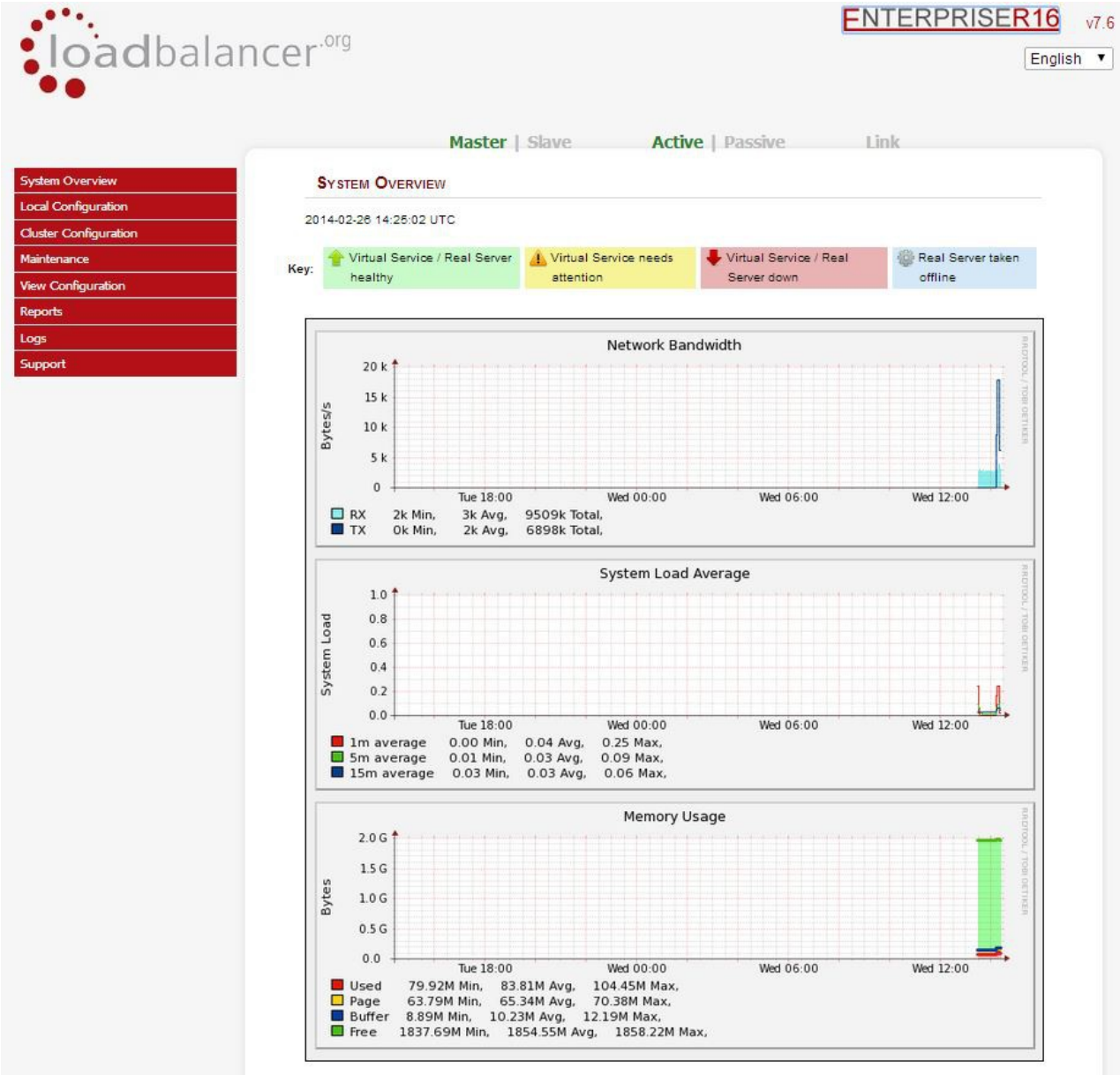
(replace 192.168.2.21 with the IP address of your load balancer if its been changed from the default)

Username: loadbalancer

Password: loadbalancer

Once you have entered the logon credentials the Loadbalancer.org Web User Interface will be displayed as shown below:

The screen shot below shows the v7.6 WUI once logged in:



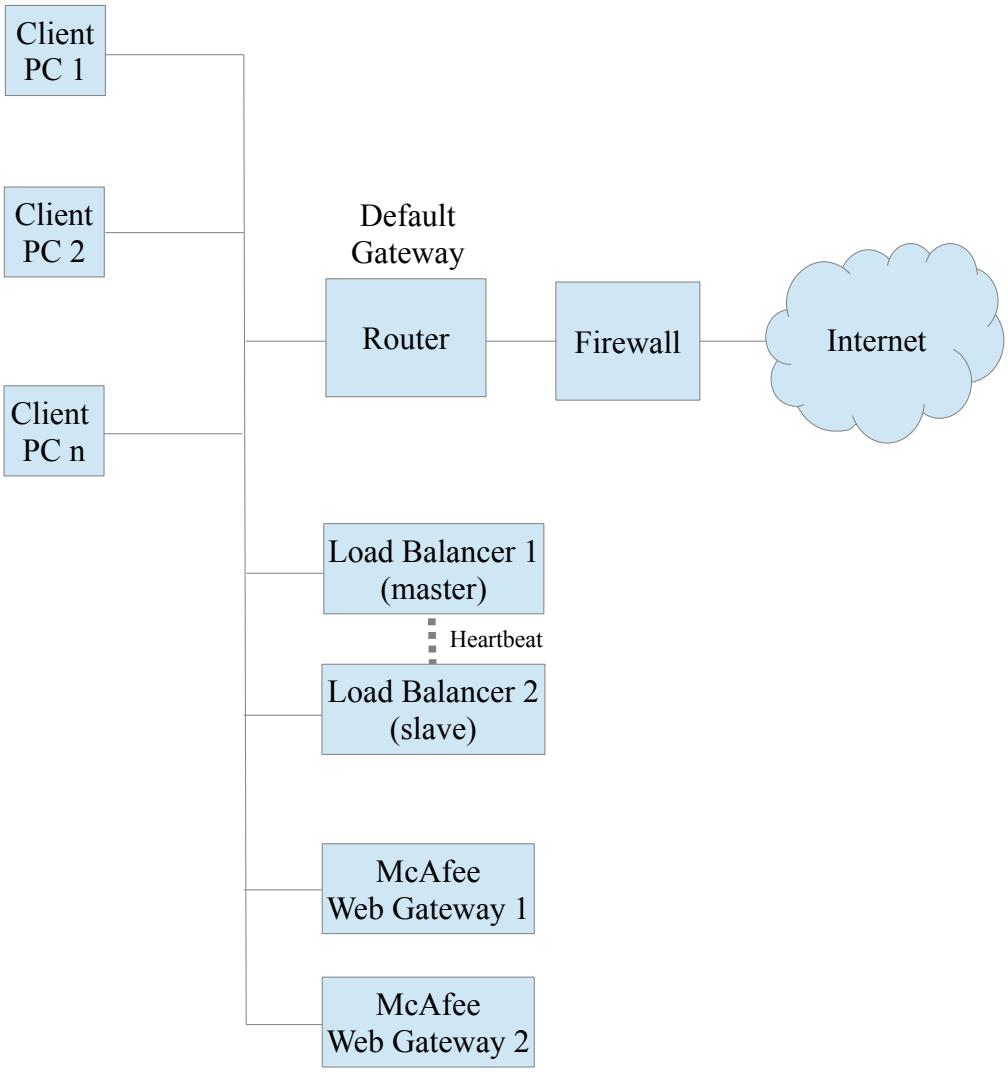
Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary slave unit is covered in section 1 of the Appendix.

NOTE: It's highly recommended that you have a working Web Gateway environment first before implementing the load balancer.

Option 1 - Proxy Mode (Recommended)

Deployment Architecture



Notes

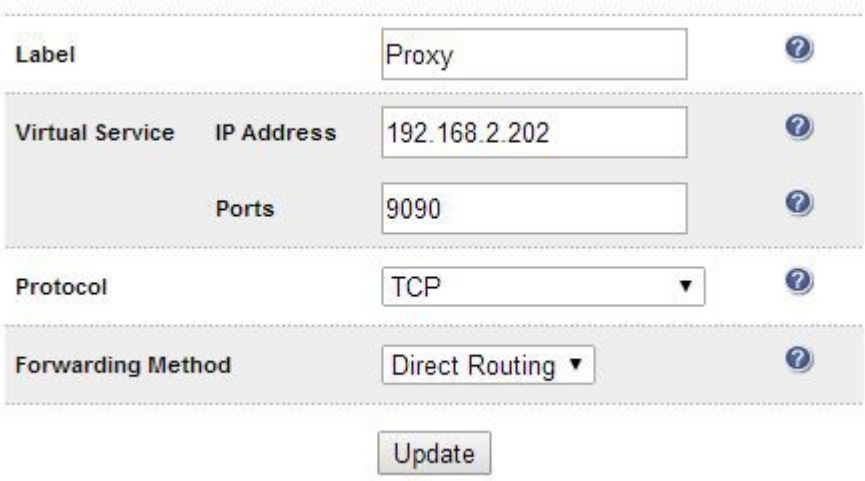
- Browser settings on client PC's must be changed to point at the Virtual Server/Service (VIP) on the load balancer
- The load balancer(s) must be configured in Layer 4 DR mode
- The McAfee Web Gateways must be configured to accept traffic for the VIP (see page 12)
- Typically, two loadbalancer.org appliances are deployed for resilience – this is our recommended configuration
- For more information on McAfee Web Gateway deployment options please refer to the following URL:

  https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24047/en_US/mwg_73_pg_product_a_en_us.pdf

Load Balancer Configuration

Create the Virtual Service (VIP)

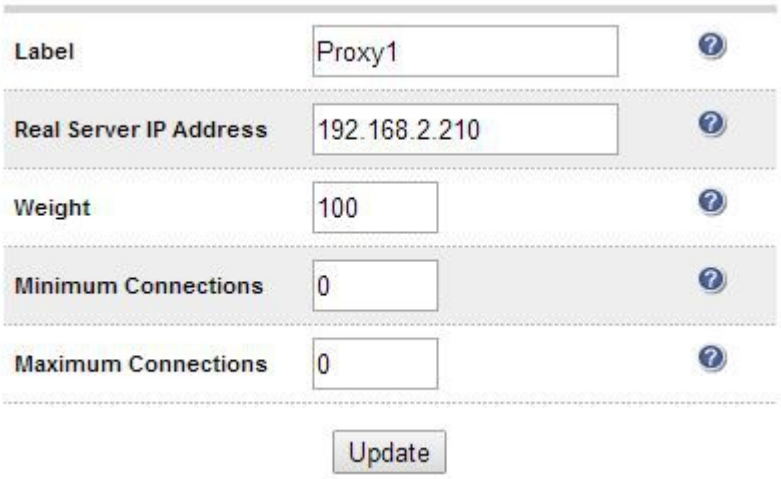
- Using the WUI go to *Cluster Configuration* > *Layer 4 – Virtual Services*
- Click **[Add a New Virtual Service]**
- Enter the following details:



- Enter an appropriate label (name) for the VIP, e.g. **Proxy**
- Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.2.202**
- Set the *Virtual Service Ports* field to the required port, e.g. **9090**
- Ensure that *Protocol* is set to **TCP**
- Ensure that *Forwarding Method* is set to **Direct Routing**
- Click **Update**
- Now click **[Modify]** next to the newly created VIP
- Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour)
- Click **Update**

Define the Real Servers (RIPs)

- Using the WUI go to *Cluster Configuration > Layer 4 – Real Servers*
- Click **[Add a new Real Server]** next to the newly created VIP
- Enter the following details:



- Enter an appropriate label (name) for the first Proxy Server, e.g. **Proxy1**
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.210**
- Click **Update**
- Repeat the above steps to add your other Web Gateway(s)

Web Gateway Configuration

Modify the Web Gateways to accept traffic for the VIP

Concept

As mentioned previously, DR mode is our recommended load balancer operating mode. To use this mode, changes are required to the real servers, i.e. the Web Gateways. The real servers must accept traffic for the VIP, but they must not respond to any ARP requests for that IP, only the VIP should do this.

To configure a Linux based Web Gateway appliance to accept traffic for the VIP the following line must be added to the rc.local startup script on each Web Gateway appliance:

iptables -t nat -A PREROUTING -p tcp -d <VIP address> -j REDIRECT

e.g.

iptables -t nat -A PREROUTING -p tcp -d 192.168.2.202 -j REDIRECT

i.e. Redirect any incoming packets destined for the VIP to the local address

N.B. For more information please refer to the administration manuals and search for 'ARP Problem'

Configuring the McAfee Appliance

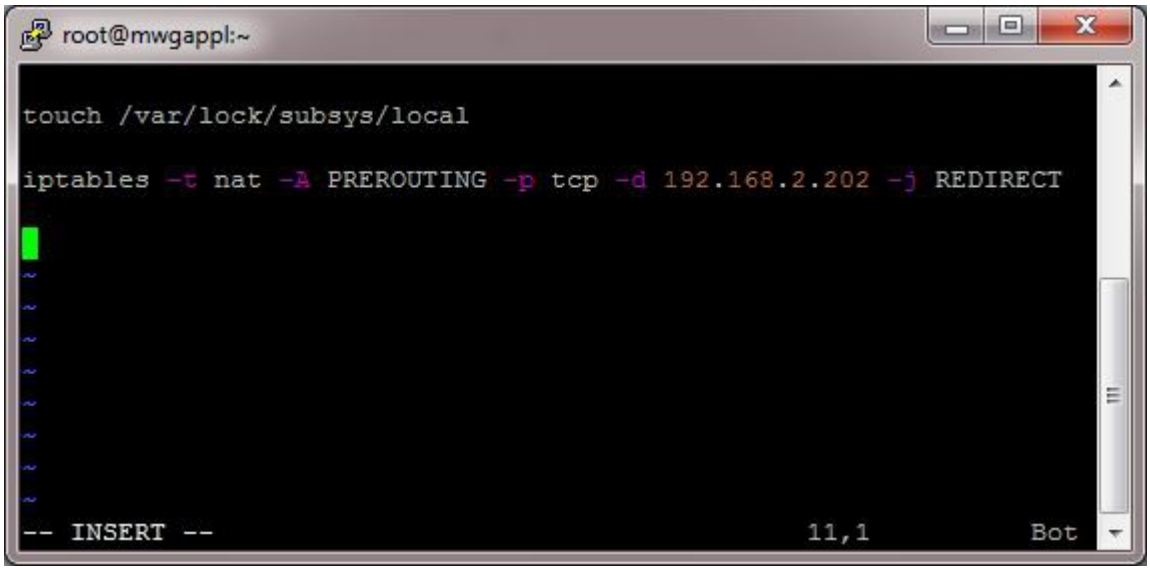
N.B. These steps must be followed on all Gateways

Login as root either at the console or using a remote ssh session

Edit the file /etc/rc.local using **vi**, **vim** or a remote editor such as the one included in WinSCP

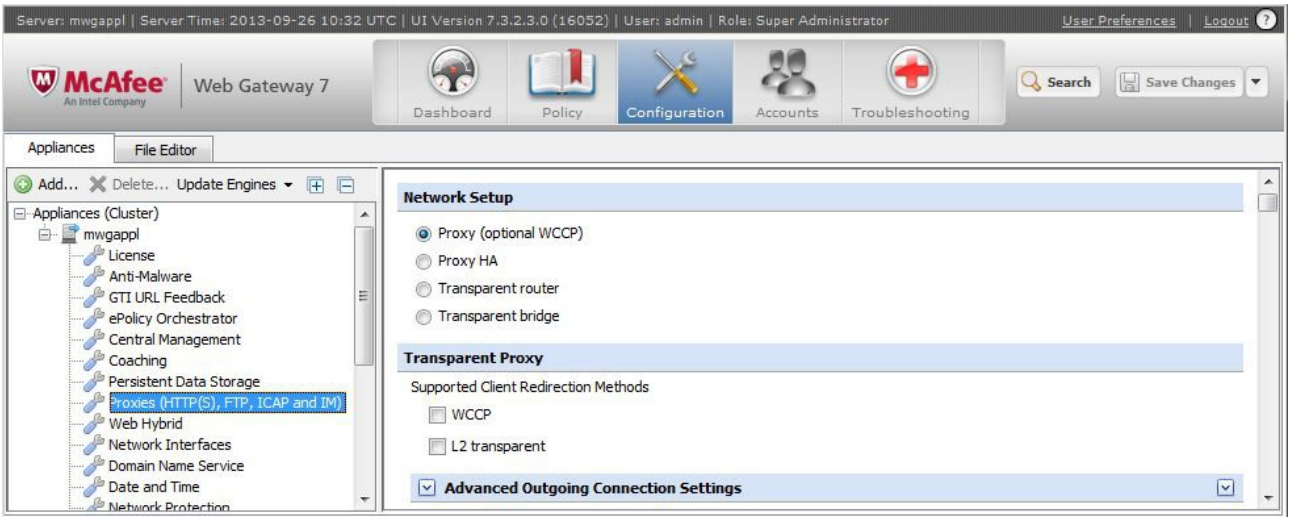
Then add the following additional line to this file as shown below:

iptables -t nat -A PREROUTING -p tcp -d <VIP address> -j REDIRECT



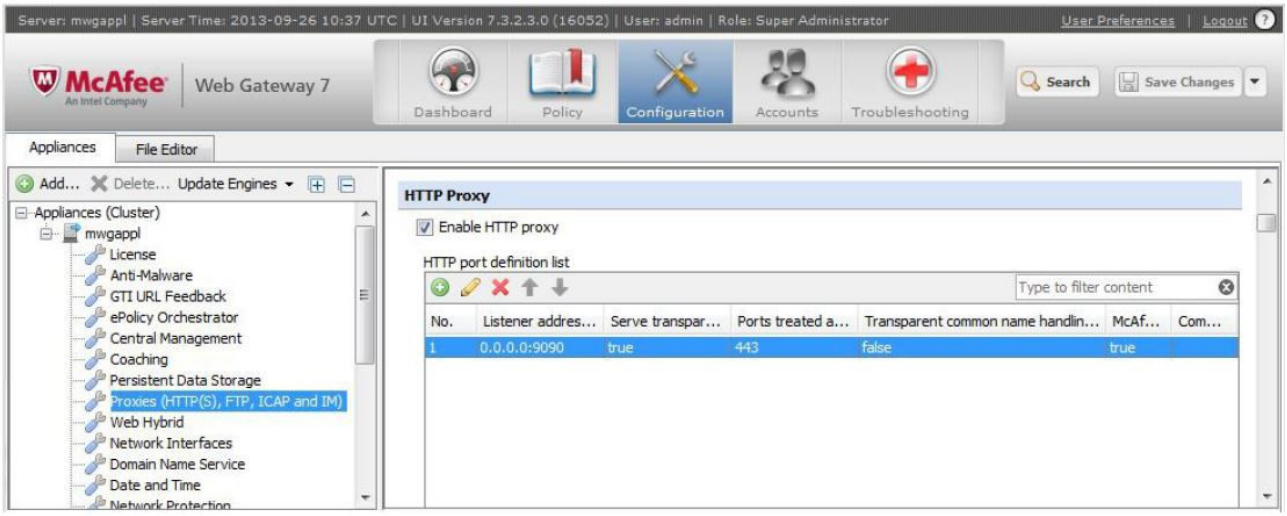
Web Gateway Operating Mode

The McAfee Web Gateway can easily be configured for proxy mode using the WUI option: *Configuration* > *Proxies (HTTP(S), FTP, ICAP and IM)* and selecting the option *Proxy (optional WCCP)* as shown below:



Proxy Port Configuration

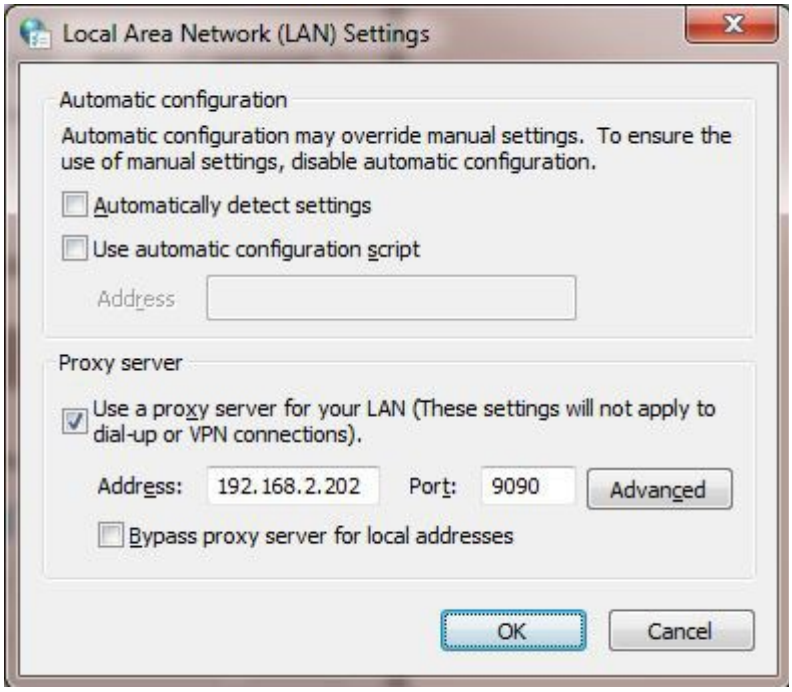
The required proxy port can be set as shown below, simple edit the default entry and change the port as required:

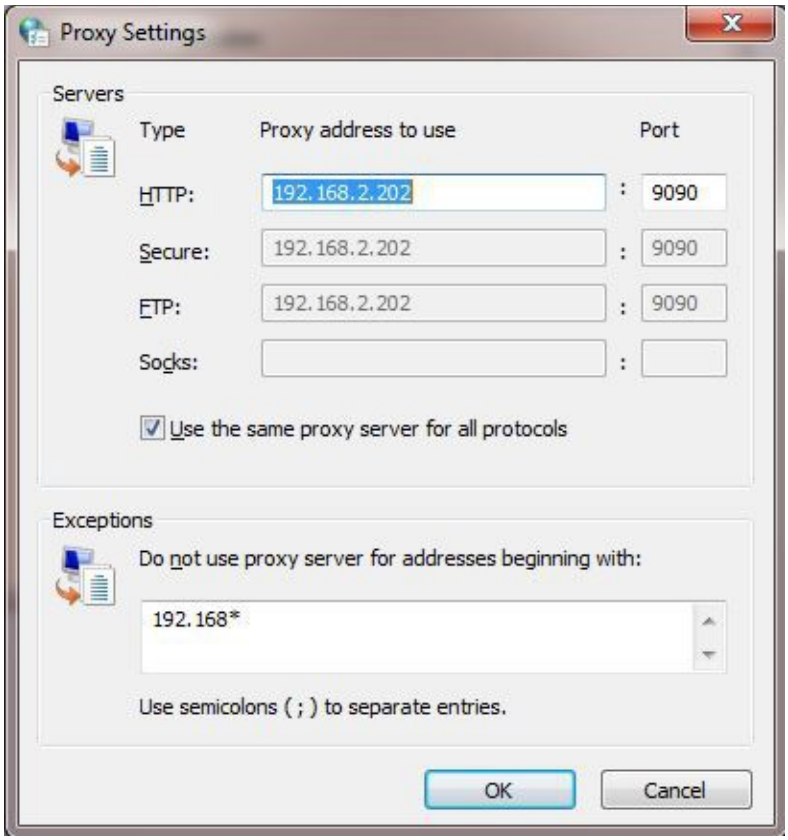


N.B. The default proxy port for McAfee Web Gateways is 9090

Client Configuration

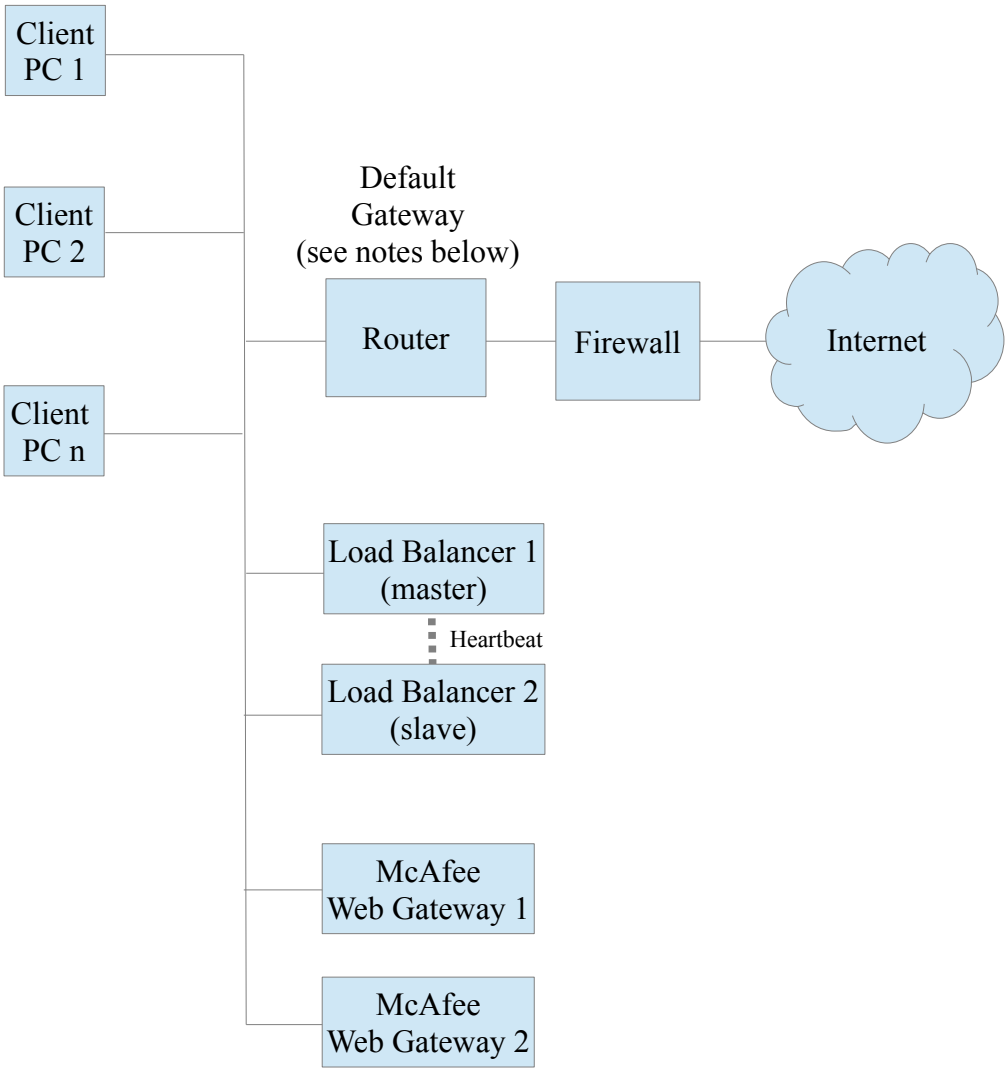
Client browser settings must be set so that browsers connect via the VIP. In a Microsoft based LAN environment, this is typically achieved using AD group policy.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 192.168.2.202
Port: 9090
Advanced
Bypass proxy server for local addresses
OK
Cancel



Option 2 - Transparent (Routed) Proxy Mode

Deployment Architecture



Notes

- If rules are added to the router so that traffic is sent transparently to the load balancer, no changes are required to client PC settings

  Alternatively, the default gateway on the client PCs should be set to be a floating IP on the load balancer (to allow master / slave failover)

- As with non-transparent mode, the load balancer is configured in Layer 4 DR mode

- Firewall rules must be added to the load balancer to transparently send traffic to the Web Gateways (see page 17)

- Typically, two loadbalancer.org appliances are deployed for resilience – this is our recommended configuration

- For more information on McAfee Web Gateway deployment options please refer to the following URL:
  https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24047/en_US/mwg_73_pg_product_a_en_us.pdf

Load Balancer Configuration

Create the Virtual Service (VIP)

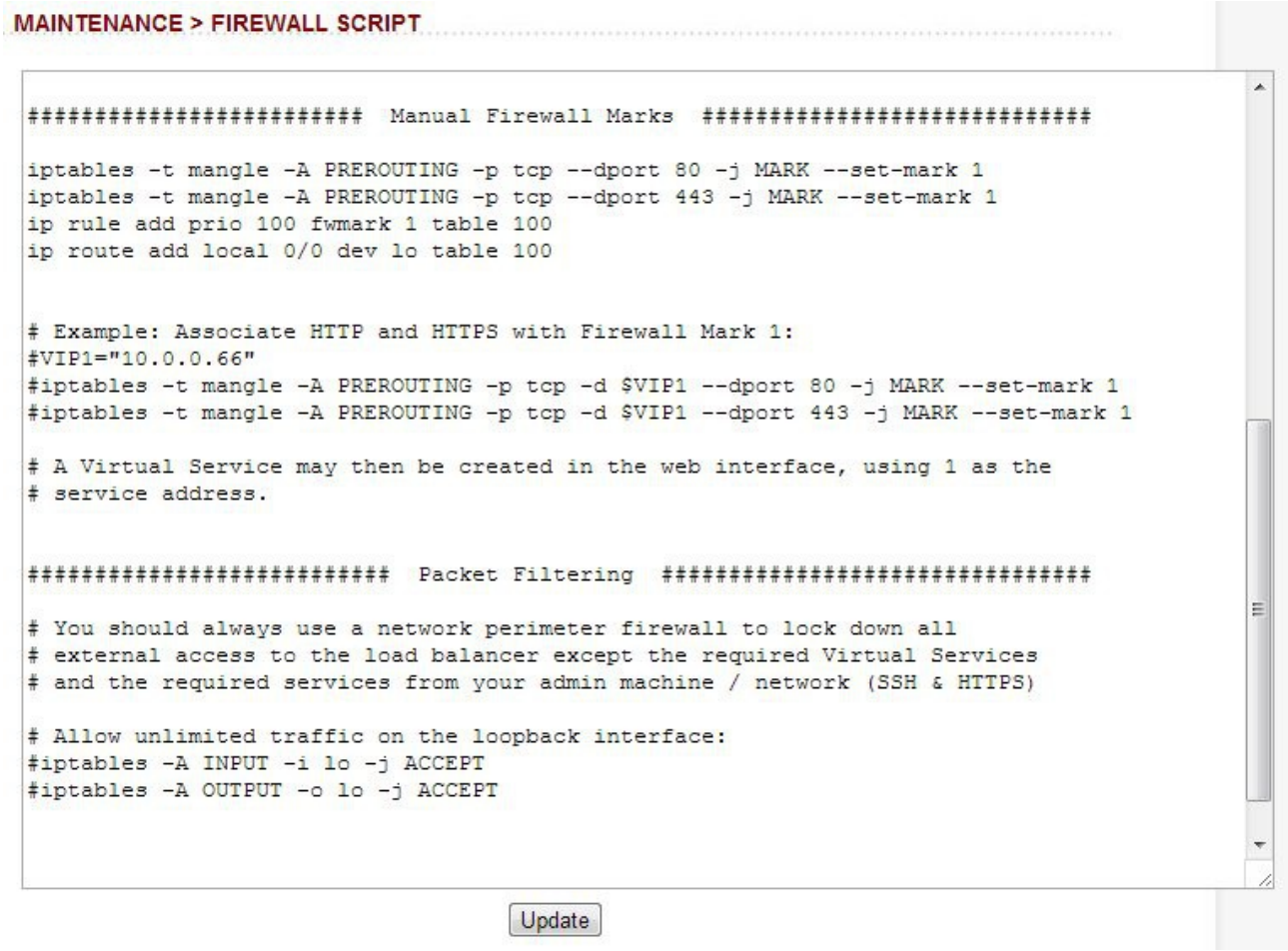
- Using the WUI go to *Cluster Configuration* > *Layer 4 – Virtual Services*
- Click **[Add a New Virtual Service]**
- Enter the following details:

- Enter an appropriate label (name) for the VIP, e.g. **Proxy**
- Change the *Virtual Service IP address* field to **1**

  N.B. This is the reference number for the 'Firewall Mark' which is required for VIPs with multiple ports – in this case, ports 80 & 443 are required. This reference number is also used when configuring the firewall rules.
- The *Virtual Service Ports* field does not need to be completed in this case and is therefore disabled
- Ensure that *Protocol* is set to **Firewall Marks**
- Ensure that *Forwarding Method* is set to **Direct Routing**
- Click **Update**
- Now click **[Modify]** next to the newly created VIP
- Ensure *Persistence* is enabled and set *Persistence Timeout* to **3600** (i.e. 1 hour)
- Under the *Health Checks* section change *Check Type* to **Ping Server**
- Click **Update**
- Using the WUI, go to *Cluster Configuration* > *Floating IPs*

- Enter an appropriate IP address for the Virtual Service, e.g. **192.168.2.202**
- Click **Update**
- Using the WUI, go to *Maintenance* > *Firewall Script*
- Scroll down to the Firewall Marks section
- Add the following lines to this section as shown in the screen shot below:

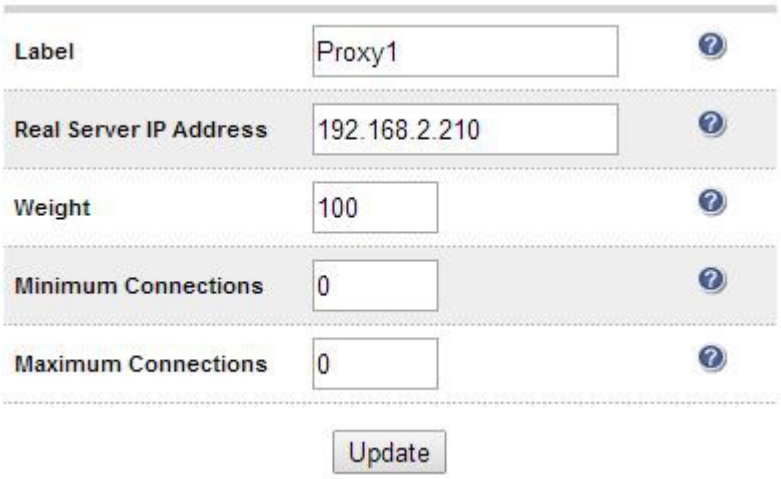
```
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
```


MAINTENANCE > FIREWALL SCRIPT
########################## Manual Firewall Marks ##############################
iptables -t mangle -A PREROUTING -p tcp --dport 80 -j MARK --set-mark 1
iptables -t mangle -A PREROUTING -p tcp --dport 443 -j MARK --set-mark 1
ip rule add prio 100 fwmark 1 table 100
ip route add local 0/0 dev lo table 100
Example: Associate HTTP and HTTPS with Firewall Mark 1:
#VIP1="10.0.0.66"
#iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 80 -j MARK --set-mark 1
#iptables -t mangle -A PREROUTING -p tcp -d $VIP1 --dport 443 -j MARK --set-mark 1
A Virtual Service may then be created in the web interface, using 1 as the
service address.
########################## Packet Filtering ###################################
You should always use a network perimeter firewall to lock down all
external access to the load balancer except the required Virtual Services
and the required services from your admin machine / network (SSH & HTTPS)
Allow unlimited traffic on the loopback interface:
#iptables -A INPUT -i lo -j ACCEPT
#iptables -A OUTPUT -o lo -j ACCEPT
Update

- Click **Update**

Define the Real Servers (RIPs)

- Using the WUI go to *Cluster Configuration > Layer 4 – Real Servers*
- Click **[Add a new Real Server]** next to the newly created VIP
- Enter the following details:



- Enter an appropriate label (name) for the first Proxy Server, e.g. **Proxy1**
- Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.2.210**
- Click **Update**
- Repeat the above steps to add your other Web Gateway(s)

Web Gateway Configuration

Web Gateway Operating Mode

The McAfee Web Gateway can easily be configured for transparent routed mode using the WUI option: *Configuration > Proxies (HTTP(S), FTP, ICAP and IM)*

Configure the following options:

1) Enable transparent router mode

2) Enable port redirection so that HTTP ports 80 & 443 are forwarded to the proxy. Also set *Director Priority* to at least 1 to enable the director

3) enable the HTTP Proxy

NOTE: When using transparent routed mode, it's not necessary to modify the Web Gateway to accept traffic destined for the VIP, this is only required when using proxy mode.

Router / Default Gateway Configuration

N.B. This is required when no changes have been made to the clients gateway settings

Depending on your network configuration, rules must be added to the router/default gateway so that all HTTP traffic is sent to the VIP on the load balancer. The load balancer then distributes this traffic between the Web Gateway servers.

Example iptables rules:

```
CLIENT="192.168.2.0/24"
FWMARK="10"
TABLE="10"
LOADBALANCER ="192.168.2.204"
iptables -t mangle -A PREROUTING -s $CLIENT -p tcp -m tcp --dport 80 -j MARK --set-mark $FWMARK
ip route flush table $TABLE
ip route add default via $LOADBALANCER dev eth3 table $TABLE
ip rule add fwmark $FWMARK table $TABLE
ip route flush cache
ip route show table $TABLE
route add default gw 192.168.2.1
```

This example uses policy routing via firewall marks. This works by first selecting and marking the packets we want to be sent to the proxy, i.e. all packets on port 80. Then, when the kernel goes to make a routing decision, the marked packets aren't routed using the normal routing table, instead via table 10 in this case. Table 10 has only one entry: route packets to the Web Gateway.

Client Configuration

If rules are configured on the router as described in the section above, no client change are required. If such rules are not configured, then the default gateway on the client PCs must be modified to be the load balancer.

Testing & Validation

To verify that the traffic is passing through the load balancer correctly the following reporting options can be used:

System Overview

Reports > Layer 4 Status

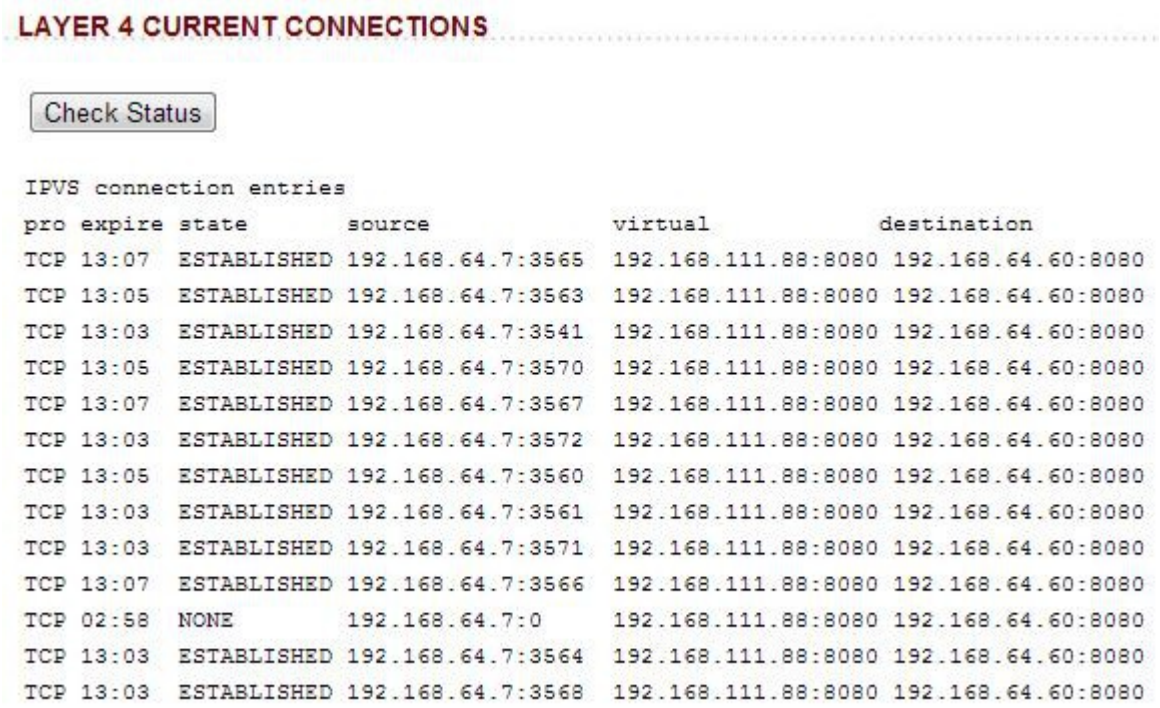
Reports > Layer 4 Current Connections

Many reporting and dashboard options are also available in the McAfee user interface. For more details please refer to the appropriate McAfee documentation

Layer 4 – Current Connections

Proxy Mode

The example screen shot below illustrates that the test client (192.168.64.7) sends requests to the VIP (192.168.111.88), the load balancer then forwards the request onto the Web Filter / Gateway (192.168.64.60).



LAYER 4 CURRENT CONNECTIONS

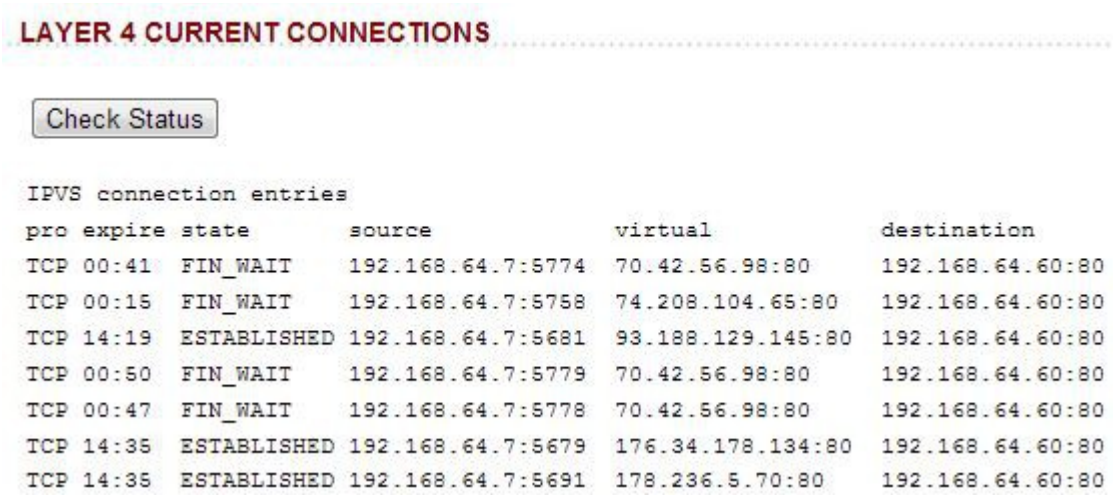
Check Status

IPVS connection entries

pro	expire	state	source	virtual	destination
TCP	13:07	ESTABLISHED	192.168.64.7:3565	192.168.111.88:8080	192.168.64.60:8080
TCP	13:05	ESTABLISHED	192.168.64.7:3563	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3541	192.168.111.88:8080	192.168.64.60:8080
TCP	13:05	ESTABLISHED	192.168.64.7:3570	192.168.111.88:8080	192.168.64.60:8080
TCP	13:07	ESTABLISHED	192.168.64.7:3567	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3572	192.168.111.88:8080	192.168.64.60:8080
TCP	13:05	ESTABLISHED	192.168.64.7:3560	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3561	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3571	192.168.111.88:8080	192.168.64.60:8080
TCP	13:07	ESTABLISHED	192.168.64.7:3566	192.168.111.88:8080	192.168.64.60:8080
TCP	02:58	NONE	192.168.64.7:0	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3564	192.168.111.88:8080	192.168.64.60:8080
TCP	13:03	ESTABLISHED	192.168.64.7:3568	192.168.111.88:8080	192.168.64.60:8080

Transparent Mode

The example screen shot below illustrates illustrates the difference when running in transparent mode.



Many reporting and dashboard options are also available in the McAfee Web Gateway user interface. For more details please refer to the appropriate McAfee documentation.

Technical Support

Loadbalancer.org support : support@loadbalancer.org

McAfee support : http://service.mcafee.com/default.aspx

Appendix

1 – Clustered Pair Configuration – Adding a Slave Unit

If you initially configured just the master unit and now need to add a slave, please refer the section 'Adding a slave unit after the master has been configured' in the administration manual which is available at the following link: http://www.loadbalancer.org/pdf/loadbalanceradministrationv7.pdf

Don't hesitate to contact our support team if you need any further assistance configuring a slave appliance: support@loadbalancer.org

2 – Loadbalancer.org Company Contact Information

Website	URL : www.loadbalancer.org
North America (US)	Loadbalancer.org, Inc. 270 Presidential Drive Wilmington, DE 19807 USA Tel : +1 888.867.9504 (24x7) Fax : +1 302.213.0122 Email (sales) : sales@loadbalancer.org Email (support) : support@loadbalancer.org
North America (Canada)	Loadbalancer.org Ltd. 300-422 Richards Street Vancouver, BC V6B 2Z4 Canada Tel : +1 855.681.6017 (24x7) Fax : +1 302.213.0122 Email (sales) : sales@loadbalancer.org Email (support) : support@loadbalancer.org
Europe (UK)	Loadbalancer.org Ltd. Portsmouth Technopole Kingston Crescent Portsmouth PO2 8FA England, UK Tel : +44 (0)330 3801064 (24x7) Fax : +44 (0)870 4327672 Email (sales) : sales@loadbalancer.org Email (support) : support@loadbalancer.org
Europe (Germany)	Loadbalancer.org GmbH Alt Pempelfort 2 40211 Düsseldorf Germany Tel : +49 (0)30 920 383 6494 Fax : +49 (0)30 920 383 6495 Email (sales) : vertrieb@loadbalancer.org Email (support) : support@loadbalancer.org

3 – McAfee Company Contact Information

Website	URL : www.mcafee.com
Worldwide Support Options	McAfee support: http://service.mcafee.com/default.aspx